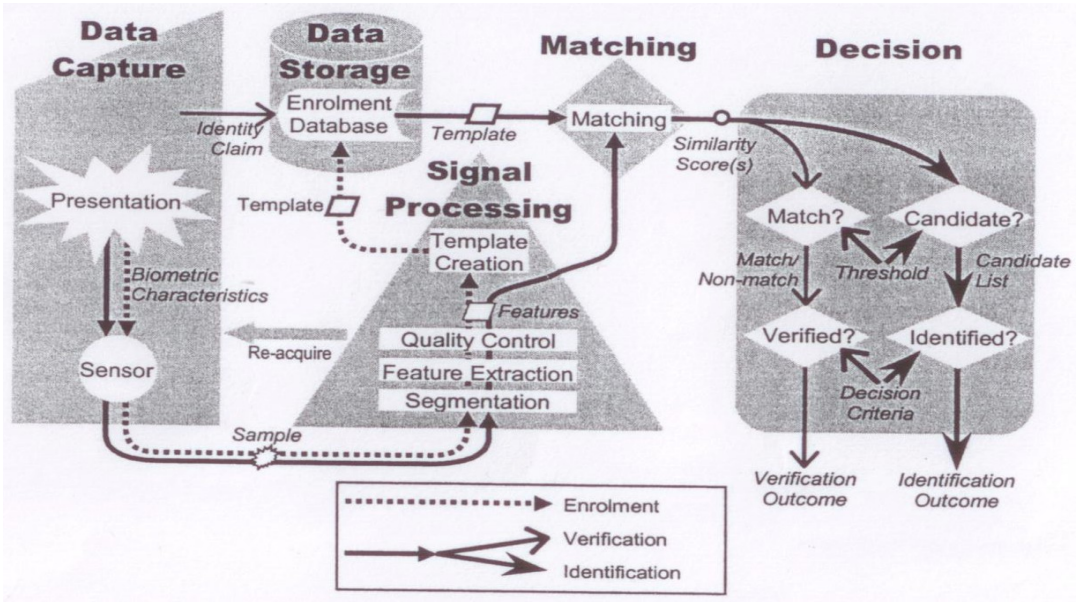
15.11.2012
Se: AFIS Praktisch hinterfragen
Dozentin: Andrea Knaut
Referenten: Marco Kähler, Marcel Zentel
Informatik in Bildung und Gesellschaft
HU Berlin

Rekapitulation, Erweiterung und Systematisierung technischer Fehler biometrischer Systeme (welche Komponenten machen welche Fehler)

1. **Anforderungen an biometrische Systeme:**
   Unisersalität, Einmaligkeit, Konstanz, **Erfassbarkeit, Leistungsfähigkeit,** Aktezptanz, Überwindungssicherheit

2. **Biometrische Systeme/Komponenten:**
   Grundlegender Aufbau:



Data Capture System, Transmission Subsystem, Single processing Subsystem, Data storage Subsystem, Matching Subsystem, Decision Subsystem, Administration Subsystem

Möglichkeiten des biometrischen Systems:
Enrolment, Verifikation, Identifikation

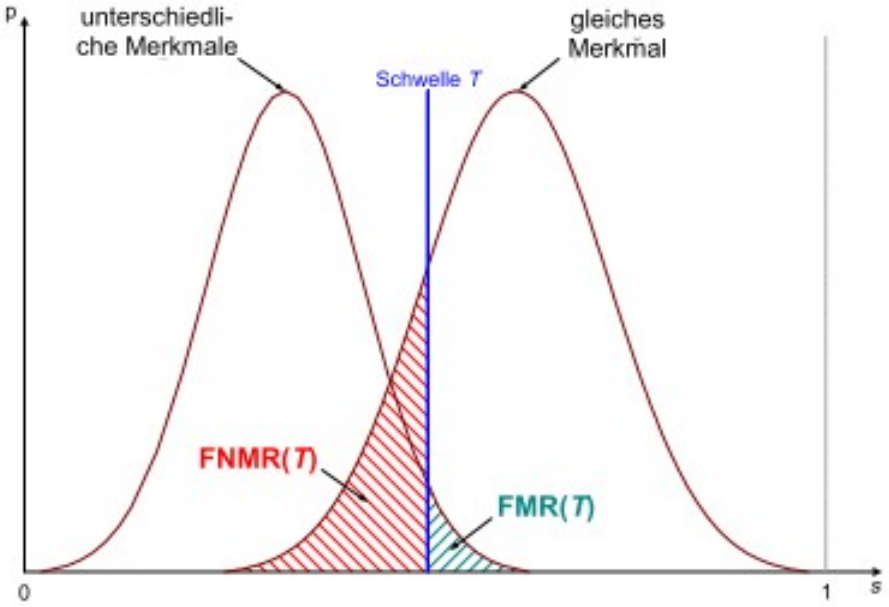
Fehler

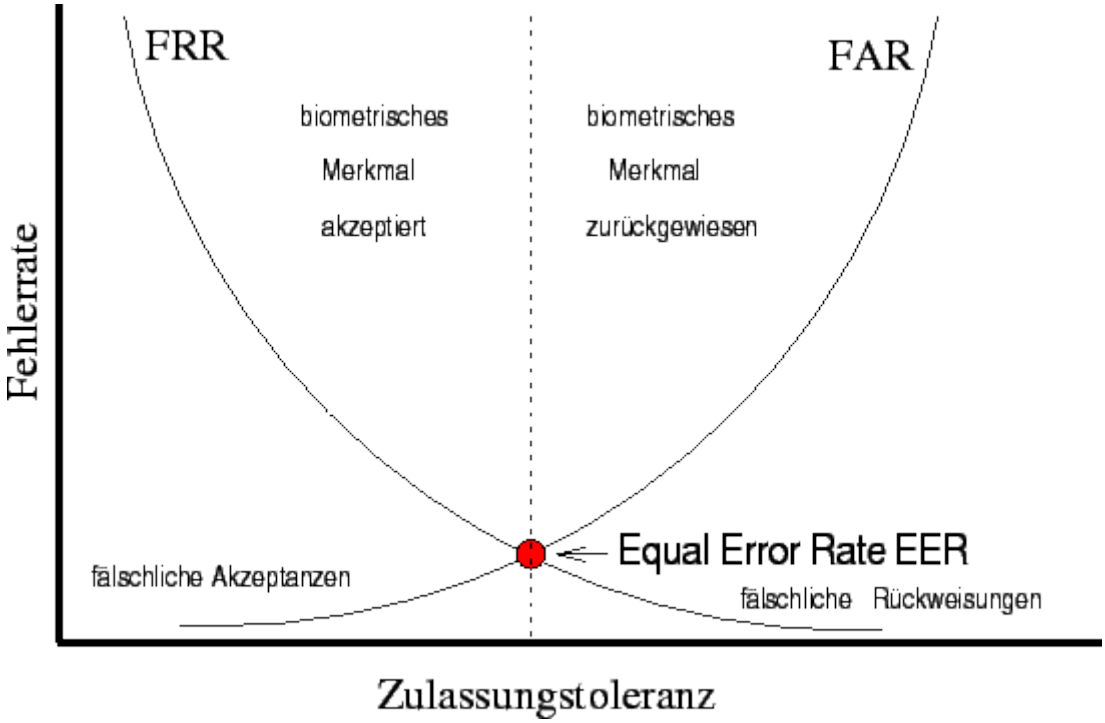
Failure-to-Acquire: FA wird nicht erkannt, obwohl auf Scanner gelegt
Failure-to-Enrol: FA konnte nicht in das System "eingelernt" werden (Qualitätskontrolle)
Failure-to-Match: FA kann wird nicht zufriedenstellend mit Templates verglichen

False Match: zwei von unterschiedlichen Fingern stammende Fingerabdrücke werden als gleich betrachtet.
False Non-Match: zwei vom gleichen Finger stammende Fingerabdrücke werden als unterschiedlich eingestuft.

$$FAR = \frac{\text{Anzahl der Vergleiche unterschiedlicher Finger, die einen Match ergeben}}{\text{Gesamtanzahl der Vergleiche unterschiedlicher Finger}}$$

$$FRR = \frac{\text{Anzahl der Vergleiche gleicher Finger, die einen Non-Match ergeben}}{\text{Gesamtanzahl der Vergleiche gleicher Finger}}$$





Falsce Acceptance und False Rejection Rate ergeben sich aus dem Schwellenwert T, der mindestens errechneten Wahrscheinlichkeit, ab dem ein Match als solches gilt. Je strikter T gesetzt wird, desto weniger False Matches, aber auch desto mehr False Rejections. Equal Error Rate bezeichnet FNMR(T) = FMR(T).

Fehlerquellen

Allgemein
Annahme: Fingerabdrücke sind individuell einzigartig
Alter & Geschlecht der Person
Fingerabdruck gefälscht (s. Experiment, CCC)
kein brauchbarer Fingerabdruck
menschliches Versagen
Wechsel bzw. Veränderungen der Algorithmen und des Equipments (Interkompatibilität)
Sensor und Algorithmus unzureichend kompatibel

Sensor & Enrolment
Noise
Störungen bei der Erfassung (Ruckeln, Schmutz)
schlechte Bildqualität (Kontrast, Auflösung)
Umwelteinflüsse (z.B. Temperatur)
bei kapazitiven Sensoren: elektrostatische Entladung
Finger falsch aufgelegt (Rotation, Position, Druck, Dauer)
Hauttypen, Beschädigungen, Trockenheit oder Feuchtigkeit der Finger

Template
Alter des templates (10 Jahre --> FRR verdoppelt)
Enrolment kann untypisch für den Finger sein
Nachbearbeitung der Bilder für Merkmalsextraktion
„Kontrast“ zwischen den Papillarlinien und den nebenliegenden Furchen
Datenbank manipuliert, falsche Templates hinterlegt

Algorithmus
Zu großer/kleiner Schwellenwert T eingestellt
Berechnung der Konfidenz eines Matchings uneindeutig
→ weder Entscheidung für Accept, noch für Reject

Szenarien für den polizeilichen Einsatz von Biometrie und deren Anforderungen in Bezug auf die Fehlerraten

1. Einsatz unterschiedlicher biometrischer Systeme zur Identitätsüberprüfung z.B. im Rahmen der Grenzkontrolle (Ein-/ Ausreisekontrolle, 1:1 Vergleich).
   FRR > FAR (FAR ≅ 0)
2. Wenn Gesichtserkennungsverfahren in der Lage sind, Gesichter von sich bewegen den Personen auch aus ungünstigen Winkeln zu erkennen und online mit vorhande nen Datenbanken abzugleichen, stellt dies neben der Auswertung von Videobändern durch biometrische Verfahren eine weitere technische Möglichkeit dar, automatisiert und zeitnah die Videoüberwachung von Brennpunkten der Kriminalität sowie besonde ren Lagen (wie nicht genehmigte Demonstrationen, Ausschreitungen bei Sportveran staltungen) effektiv zu unterstützen (1:n-Fahndungsszenario).
   FRR < FAR
3. Biometrischer Abgleich von Gesichtsaufnahmen mit Phantombildern (1:n).
   FRR < FAR
4. Mobiler Einsatz von Fingerabdruckscannern (Personenkontrolle vor Ort, 1:n).
   FRR < FAR

5. ED-Maßnahmen mittels biometrischem Fingerabdruckscan und Abgleich mit AFIS (1:n).

FRR < FAR

6. Identifizierung von Wiederholungstätern anhand biometrischer Merkmale wie Stimme und Gang (z.B. über Videoaufnahmen von Banküberfällen, 1:n).

FRR < FAR

Während im ersten Szenario eine weitergehende Ergebnisüberprüfung des biometrischen Vergleichs in der Regel nicht erfolgt, können die Resultate der biometrischen Systeme in den Szenarien 2 bis 6 lediglich als Ermittlungsansätze bzw. Hinweise dienen, die in jedem Fall durch weitere Maßnahmen, z.B. den Einsatz eines kriminaltechnischen Sachverständigen, verifiziert werden müssen.

Quellen:

http://www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/04Fingerprint/fingerabdrucksysteme.pdf
http://vds.de/fileadmin/vds_publikationen/vds_3112_web.pdf
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioFinger/BioFinger_I_I_pdf.pdf?__blob=publicationFile
https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/biop/BioPII.html